NAS-IR-51070000
05/28/97

DEPARTMENT of TRANSPORTATION

Federal Aviation Administration

Interface Requirements Document

NAS Infrastructure Management System Manager/
Managed Subsystem

INTERFACE REQUIREMENTS DOCUMENTS
APPROVAL SIGNATURE PAGE

NAS Infrastructure Management System (NIMS) Manager/
Managed Subsystem

APPROVAL SIGNATURES		
PARTICIPANT	NAME	DATE
ASD-100	John C. Arguelles	7/9/97
AND-100	Jeffrey L. Brown	7/9/97
AOP-300	Michael S. Hoffman	7/14/97

CONTENTS

CONTENTS (cont.)

FIGURES

TABLES

1. SCOPE

1.1 Scope.

This Interface Requirements Document (IRD), is prepared in accordance with FAA-STD-025d. It provides interface requirements to enable the Federal Aviation Administration (FAA) National Airspace System Infrastructure Management System (NIMS) Managers to remotely monitor and control Managed Subsystems (i.e., NAS Subsystems designated to be managed by the NIMS Manager). NIMS Manager will manage the NAS Subsystems by sending management operations to and receiving notifications from the NIMS Agents. Therefore, this IRD specifies interface requirements between the NIMS Manager and the NIMS Agent.

The interface will be based on industry open system management standards which include, but is not limited to the Simple Network Management Protocol Version 1 (SNMPv1), SNMPv2, and the Common Management Information Protocol (CMIP).

This IRD is the basis for generic NIMS interface control documents (ICD) which will define how the interface requirements specified in this IRD are to be met using SNMPv1, SNMPv2, CMIP, and other standard management protocols approved by the NIMS Product Team (PT).

The generic NIMS ICDs will enable the development of NAS Subsystem specific ICDs which would be approved by the NAS Subsystem Integrated Product Team (IPT) and the NIMS PT. If a capability required in this document is not available, a viable alternative may be provided, once agreed to by the NAS Subsystem IPT and the NIMS PT.

1.2 Subsystem responsibility list.

Subsystem/Equipment	Common Name	Office (TBR)
NIMS Manager	NIMS Manager	NIMS Product Team
NAS Subsystem	NIMS Agent	NAS Subsystem Product Team

2. APPLICABLE DOCUMENTS

The following documents form a part of this IRD to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this IRD, the contents of this IRD shall be the superseding requirements.

2.1 Government Documents.

Federal Aviation Administration Specifications

FAA-E-2911:1997	System Level Specification for NAS NIMS Managed Subsystems
FAA-E-2912:1997	System Level Specification for the NAS Infrastructure Management System

Federal Aviation Administration Standards

FAA-STD-025d:1995	Preparation of Interface Documentation
FAA-STD-039b:1996	Open Systems Architecture and Protocols
FAA-STD-043b:1996	Open System Interconnection Priority
FAA-STD-045:1994	OSI Security Architecture, Protocol and Mechanisms
FAA-HDBK-002:1997	Open Systems Management

Other FAA Documents

NAS-IC-43020001:1996	NADIN PSN X.25 Packet Mode Users Interface Control Document
NAS-IR-40010001:1995	NAS LAN Users Systems Interface Requirements Document

2.2 Non-government documents.

International Organization for Standardization (ISO)

ISO 7498: 1984	Information Processing Systems - Open Systems Interconnection - Part: Basic Reference Model
ISO :8824:1987	Information Processing Systems - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1)
ISO 8825:1987	Information Processing Systems - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)

2.3 Document sources.

2.3.1 Source of FAA Documents.

Copies of FAA specifications, standards, and publications may be obtained from the Contracting Officer, Federal Aviation Administration, 800 Independence Avenue, S.W., Washington, D.C., 20591. Requests should clearly identify the desired material by number and date, and state the intended use of the material.

2.3.2 ISO Documents.

Copies of ISO standards may be obtained from the American National Standards Institute, 11 West 42nd Street, New York, NY, 10036.

3. INTERFACE REQUIREMENTS

3.1 General requirements.

This IRD describes the interface requirements between the NAS Infrastructure Management System (NIMS) Manager and NIMS Agents. The agent may be an embedded agent, proxy agent, or proxy agent/concentrator.

a) The connectivity between the NIMS Manager and the NIMS Agent shall enable NIMS to monitor and control NAS Subsystems as shown in Figure 3-1. [NOTE: Connectivity between the NIMS Manager and NIMS Agent may include point-to-point, local area networks (LAN), and/or wide area networks (WAN).]

b) Proxy agents shall be used to allow NAS subsystems, using proprietary and non-standard management functions (e.g., NAS-MD-790), to communicate with the NIMS Manager.

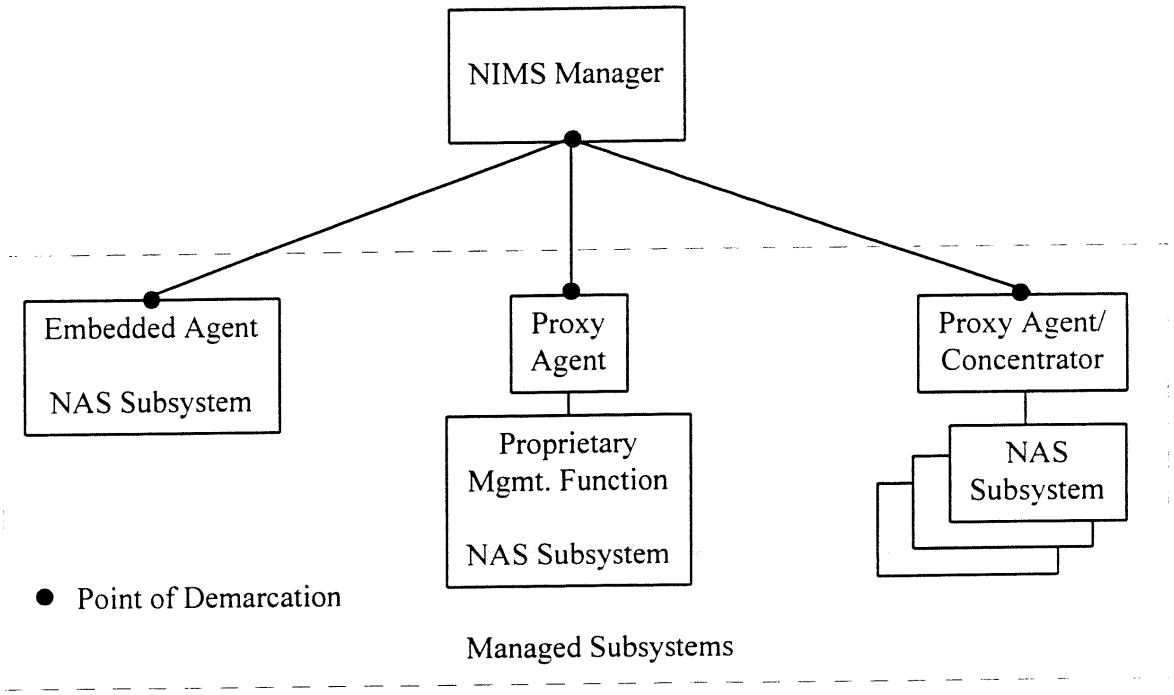

Figure 3-1. NIMS Functional Connectivity

3.2 Functional requirements.

a) The functional interface between the NIMS Manager and the NIMS Agent shall use layered protocols which provide peer-to-peer communication as defined in ISO 7498: International Organization for Standardization (ISO) Open Systems Interconnection (OSI) Reference Model and illustrated in Figure 3-2.

b) The functional interface requirements provided in this section shall be implemented in accordance with one of several NIMS PT approved ICDs.

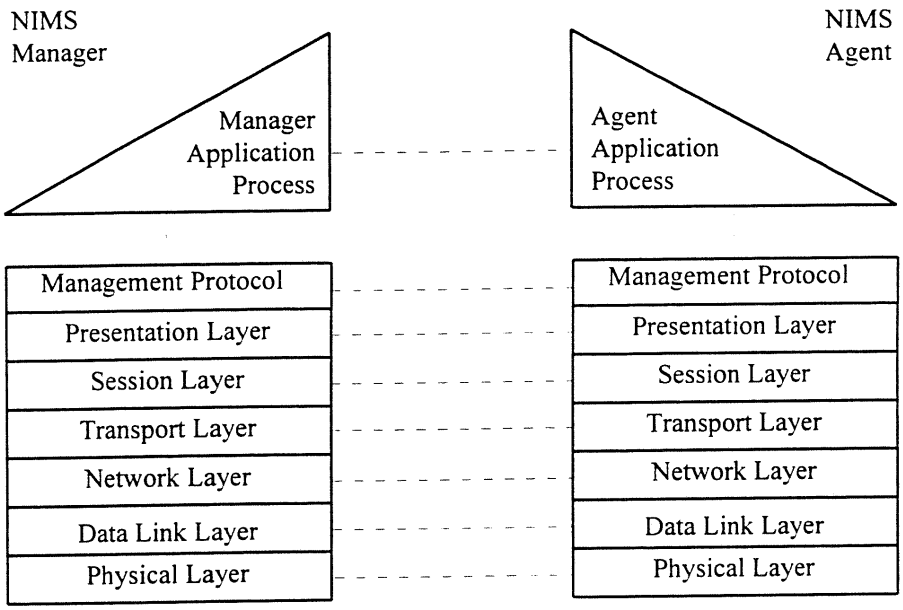

Figure 3-2. NIMS Manager/Agent Interface

3.2.1 Application process.

3.2.1.1 Identification of application process.

a) The application which implement manager monitor and control requirements specified in the System Level Specification for the NAS Infrastructure Management System, FAA-E-2912, shall be identified as the NIMS Manager application process (AP).

b) The application which implements the applicable monitor and control requirements specified in the System Level Specification for NIMS Managed Subsystems, FAA-E-2911, shall be identified as the NIMS Agent AP.

3.2.1.2 Type of services required by the AP.

a) Reliable event reporting, solicited data reporting, and control services shall be provided in accordance with the open systems management standard(s) identified in the NIMS-approved ICD that is applicable to a particular interface.

3.2.1.2.1 Event reporting.

a) The NIMS Agent shall send notifications, to the NIMS manager, indicating occurrence of events within the NAS subsystem.

b) Events shall include, but are not limited to, the following types:

- Operating Status Change
- Administrative State (Operating Mode) Change
- Configuration Change
- Performance Threshold Transition
- Access Control Rule Violation

3.2.1.2.2 Solicited data reporting.

a) The NIMS Manager shall be able to request management data from the NIMS Agent.

b) Solicited data shall include, but is not limited to, the following types:

- Monitored attributes
- Control attributes
- Security log data

c) The NIMS Agent shall respond by sending the solicited data.

3.2.1.2.3 Control.

3.2.1.2.3.1 Initiate action.

a) The NIMS Manager shall be able to invoke actions to be performed by the NIMS Agent.

b) Requested actions shall include, but are not limited to the following:

- Reset Subsystem
- Perform Diagnostics

c) The NIMS Agent shall report the result(s) and/or completion of actions to the NIMS Manager.

3.2.1.2.3.2 Modify managed resource attributes.

a) The NIMS Manager shall be able to request the modification of managed resource attributes by the NIMS Agent.

b) Managed resource attributes shall included, but is not limited to, the following:

- Automatic Fault Isolation Parameters
- Fault Recovery Processing Parameters
- Event Forwarding Discriminators
- Fault Management Threshold
- Administrative State
- Configuration Attributes
- Performance Thresholds
- Access Control Rules

c) The NIMS Agent shall respond by sending the modified managed resource attribute to the NIMS Manager.

3.2.1.3 Information units.

a) Management information shall be exchanged between the NIMS Manager and NIMS Agent using information units defined in the open system management standard(s) referenced in the NIMS-approved ICD selected for the interface.

b) NIMS Manager and NIMS Agent information units shall be formatted in accordance with the open system management standard(s) referenced in the NIMS-approved ICD selected for the interface.

3.2.1.3.1 Information code.

a) The management information transferred between the NIMS Manager and NIMS Agent shall be defined, using an abstract syntax, in accordance with the open system management standard(s) referenced in the NIMS-approved ICD selected for the interface, e.g., ISO 8824: Abstract Syntax Notation One (ASN.1).

b) The management information shall be encoded, for data transfer, in accordance with the open system management standard(s) referenced in the NIMS-approved ICD selected for the interface, e.g., ISO 8825: Basic Encode Rules (BER) for ASN.1.

3.2.1.3.1.1 Protocol data unit.

a) The management information shall be transferred between the NIMS Manager and NIMS Agent using protocol data units (PDU) in accordance with the open systems management standard(s) referenced in the NIMS-approved ICD selected for the interface.

3.2.1.3.2 Information structure.

a) The management information base (MIB), which provide logical the definition and structure of NAS Subsystem resources, shall be structured in accordance with the open systems management standard(s) referenced in the NIMS-approved ICD selected for the interface.

b) The MIB structure shall allow private extensions, e.g., NIMS MIB, vendor MIBs. in accordance with the open systems management standard(s) referenced in the NIMS-approved ICD selected for the interface.

c) The NIMS Manager and NIMS Agent shall support the standard MIBs provided in the open systems management standard(s) referenced in the NIMS-approved ICD selected for the interface.

d) The NIMS Manager and NIMS Agent shall support applicable private MIB structured in accordance with the open systems management standard(s) referenced in the NIMS-approved ICD selected for the interface.

e) The MIB naming plan shall be in accordance with FAA guidance and the open system standard(s) referenced in the NIMS-approved ICD selected for the interface.

3.2.1.3.3 Information unit segmentation.

a) The maximum information unit size shall be in accordance with the applicable open system management standard(s) referenced in the NIMS-approved ICD selected for the interface.

3.2.1.3.4 Information flow.

a) The information flow shall be as described in Table 3-1.

b) Event reports shall be provided by the NIMS Agent.

c) The request for management data shall be provided by the NIMS Manager.

d) Solicited management data shall be provided by the NIMS Agent.

e) Control operations shall be requested by the NIMS Manager.

f) Confirmation of the completion of control operations shall be provided by the NIMS Agent.

3.2.1.3.5 Frequency of transmission.

a) The NIMS Agent shall report events to the NIMS Manager as they occur.

b) The NIMS Manager shall request management data from the NIMS Agent at a frequency agreed upon by the FAA.

c) The NIMS Manager shall send control commands to the NIMS Agent as needed.

3.2.1.4 Interface summary table.

a) A summary of the messages to be exchange across the interface is provided in Table 3-1. This interface shall provide the ability to transfer the listed messages between application processes.

3.2.1.5 Quality of service.

3.2.1.5.1 Information priority.

a) Management information shall be communicated as the highest priority data in accordance with FAA-STD-043: Open System Interconnection Priority.

3.2.1.5.2 Information security.

a) Information security provided by the NIMS Manager and the NIMS Agent shall include, but is not limited to, the following:

- Access control
- Data origin authentication

3.2.1.6 AP Error handling.

a) The NIMS Manager and NIMS Agent shall process errors received from protocol operations, which may include but are not limited, to the following:

- PDU too large
- No such name
- Bad value
- Read only
- General error

Table 3-1. NIMS Manager/NIMS Agent Interface Summary.

A NIMS Manager	B Message	Direction	C NIMS Agent
Event Reporting Service	Operating Status Change	A<-C	Event Reporting Service
	Operating Mode Change	A<-C	
	Configuration Change	A<-C	
	Performance Transition	A<-C	
	Access Control Rule Violation	A<-C	
Solicited Data Report Service	Report Monitored Attribute	A->C	Solicited Data Report Service
	Monitored Attributes	A<-C	
	Report Control Attributes	A->C	
	Control Attributes	A<-C	
	Report Security Logs	A->C	
	Security Logs	A<-C	
Control Service-Action	Reset Subsystem	A->C	Control Service-Action
	Confirmation	A<-C	
	Perform Diagnostics	A->C	
	Confirmation	A<-C	
Control Service - Modify	Automatic Fault Isolation Parameters	A->C	Control Service - Modify
	Confirmation	A<-C	
	Fault Recovery Processing Parameters	A->C	
	Confirmation	A<-C	
	Event Forwarding Discriminators	A->C	
	Confirmation	A<-C	
	Fault Management Threshold	A->C	
	Confirmation	A<-C	
	Administrative State	A->C	
	Confirmation	A<-C	
	Configuration Attributes	A->C	
	Confirmation	A<-C	
	Performance Thresholds	A->C	
	Confirmation	A<-C	
	Access Control Rules	A->C	
	Confirmation	A<-C	

3.2.2 Communications requirements.

FAA guidance on using standards specified in this section is provided in FAA-HDBK-002: Open Systems Management and FAA-STD-039: Open Systems Architecture and Protocols. Specific aspects of these guidance documents are cited as appropriate in the NIMS-approved ICDs.

3.2.2.1 Application layer.

a) The application layer protocol(s) for providing communication of management information shall be in accordance with FAA guidance and open system management standards(s) referenced in the NIMS-approved ICD selected for the interface.

b) The application layer protocol(s) for providing loop-back testing shall be in accordance with FAA guidance and open system management standards(s) referenced in the NIMS-approved ICD selected for the interface.

3.2.2.2 Presentation layer.

a) Applicable presentation layer protocol(s) shall be in accordance with FAA guidance and open system management standards(s) referenced in the NIMS-approved ICD selected for the interface.

3.2.2.3 Session layer.

a) Applicable session layer protocol(s) shall be in accordance with FAA guidance and open system management standards(s) referenced in the NIMS-approved ICD selected for the interface.

3.2.2.4 Transport layer.

a) Applicable transport layer protocol(s) shall be in accordance with FAA guidance and open system management standards(s) referenced in the NIMS-approved ICD selected for the interface.

3.2.2.5 Network layer.

a) Applicable network layer protocol(s) shall be in accordance with FAA guidance and open system management standards(s) referenced in the NIMS-approved ICD selected for the interface.

3.2.2.6 Addressing.

a) Addressing shall be in accordance with FAA guidance and open system management standards(s) referenced in the NIMS-approved ICD selected for the interface.

3.2.2.7 Subnetwork profile 1: point-to-point interface.

a) Point-to-point connections shall be provided in accordance with FAA guidance and open system management standards(s) referenced in the NIMS-approved ICD selected for the interface.

3.2.2.7.1 Dedicated connection.

a) The NIMS Agent shall be responsible for initiating the connection when dedicated communication services are used.

b) The NIMS Manager and the NIMS Agent shall maintain continuous connection.

c) In the event of disconnection, e.g., due to the NIMS Manager or NIMS Agent internal processing such as shut down, restart, communication loss, etc., the NIMS Agent shall initiate a connection establishment procedure.

3.2.2.7.2 Dial-up connection.

a) The NIMS Manager shall be able to establish a connection with the NIMS Agent over a dial-up telephone line.

b) When called over its dial up connection, the NIMS Agent shall authenticate the originator of the data in accordance with FAA guidance or open system management standards(s) referenced in the NIMS-approved ICD selected for the interface.

c) The NIMS Agent shall be able to establish a connection with the NIMS Manager over a dial-up connection.

d) When called over its dial up connection, the NIMS Manager shall authenticate the originator of the data in accordance with FAA guidance or open system management standards(s) referenced in the NIMS-approved ICD selected for the interface.

e) The originator of the call shall be capable of terminating the connection after an operationally specified period of inactivity on the circuit.

3.2.2.8 Subnetwork profile 2: local area network interface.

a) NAS Local area network (LAN) interfaces shall be in accordance with NAS-IR-4001000: NAS LAN/User Systems Interface Requirements Document and FAA guidance.

3.2.2.9 Subnetwork profile 3: wide area network interface.

a) Interfaces to the National Data Interchange Network (NADIN) Packet Switching Network (PSN) shall be in accordance with NAS-IC-43020001: NADIN PSN X.25/Packet Mode User Interface Requirements Document and FAA guidance.

3.3 Security.

a) Security requirements shall be in accordance with FAA-STD-045: OSI Security Architecture, Protocol and Mechanisms or its revision.

4. QUALITY ASSURANCE PROVISIONS

4.1 General.

Verification shall be in accordance with Table 4-1, Verification Requirements Traceability Matrix (VRTM). The verification levels and methods used in this IRD are presented below.

4.2 Special verification levels and methods.

There are no special verification requirements imposed by this IRD.

4.3 Verification levels and methods.

There are three basic levels of verification. All requirements imposed by section 3 of the IRD shall be verified at one or more of the following three levels:

a) Subsystem Level. This level of verification is usually accomplished by the subsystem's contractor testing with the FAA test support operating the interfacing subsystem during testing. The contractor shall determine in the test planning documentation the allocation (factory, site) of the test requirements identified in the VRTM. The contractor's completion of validating all elements of VRTM culminates in the formal qualification of the interface end-item.

b) Integration Level. This level of verification is conducted by the FAA after interface qualification and acceptance testing from the contractor and during Operational Testing and Engineering (OT&E)/Integration testing. This testing is also identified as FAA end-to-end testing. The OT&E/Integration test plan shall determine the location for testing, e.g., FAA Technical Center, Test site.

c) Site Level. This level of verification is usually performed at the designated site. The verification portion of the subsystem installation and checkout shall emphasize the demonstration of the overall system, the final acceptance demonstrations, and commissioning activities. All verification levels for subsystem to facilities interface would normally occur at the installation site.

4.4 Quality conformance inspections.

The VRTM presented in Table 4-1 lists the requirements to be verified, the phase or levels at which verification shall occur, and the method of verification that shall be used.

4.5 Verification requirements.

Compliance with the requirements stated in the IRD are deemed met when all the requirements specified in a paragraph are verified by one or more of the methods outlined in the subsequent subparagraphs. The results of the verification activities shall be expressed as either pass or fail.

4.6 Verification methods.

There are four verification methods that can be used at any of the three verification levels. Verification methods are:

a) Analysis. This method of verification consists of comparing hardware or software design with known scientific and technical principles, procedures, and practices to estimate the capability of the proposed design to meet the mission and system requirements. When certain elements of design are comprised of previously qualified elements such as commercial off the shelf (COTS) equipment, then analysis of previous qualification testing in meeting specification requirements may be used to reduce the amount of qualification testing.

b) Demonstration. Demonstration is a method of verification where qualitative determination of properties is made for configuration items, including software, and/or technical data and documentation measured, in a dynamic state.

c) Inspection. Inspection is a method of verification to determine compliance without the use of special test equipment, procedures, or services, and consist of a non-destructive static-state examination of the hardware, software, and/or the technical data and documentation.

d) Test. Test is a method of verification wherein performance is measured during or after the controlled application of functional and/or environmental stimuli. Quantitative measurements are analyzed to determine the degree of compliance to the success criteria stipulated in the IRD or project specification. The process uses standardized laboratory equipment, procedures, hardware, and/or services.

Table 4-1. Verification Requirements Traceability Matrix

(Verification Methods: D - Demonstration, I - Inspection, A - Analysis, T - Test, X - Not Applicable)

Section 3	Requirements	Verification Phase and Method			
		Sub-system Level	Integration Level	Site Level	Remarks
3.	INTERFACE REQUIREMENTS				Title
3.1	General Requirements	D	D	D	
3.1a	Functional connectivity	D	D	D	
3.2b	NIMS Proxy Agent	D	D	D	
3.2	Functional Requirements				Title
3.2a	Manager/agent interface	D	D	D	
3.2b	IAW interface control document	D	D	D	
3.2.1	Application Process				Title
3.2.1.1	Identification of application process				Title
3.2.1.1a	Manager application process	D-I	D-I	D	
3.2.1.1b	Agent application process	D-I	D-I	D	
3.2.1.2	Type of service required by the AP	D	D	D	
3.2.1.2a	Reliable services	D	D	D	
3.2.1.2.1	Event reporting				Title
3.2.1.2.1a	Event notification	D-T	D-T	D	
3.2.1.2.1b	Event type	D-T	D-T	D	
3.2.1.2.2	Solicited Data Reporting				Title
3.2.1.2.2a	Solicit data	D-T	D-T	D	
34.2.1.2b	Data type	D-T	D-T	D	
3.2.1.2.2b	Response to request	D-T	D-T	D	
3.2.1.2.3	Control				Title
3.2.1.2.3.1	Initiate action				Title
3.2.1.2.3.1a	Invoke action	D-T	D-T	D	
3.2.1.2.3.1b	Requested actions	D-T	D-T	D	
3.2.1.2.3.1e	Action completion report	D-T	D-T	D	
3.2.1.2.3.2	Modify managed resource attributes				Title
3.2.1.2.3.2a	Modification request	D-T	D-T	D	
3.2.1.2.3.2b	Resources attributes	D-T	D-T	D	
3.2.1.2.3.2c	Modification response	D-T	D-T	D	
3.2.1.3	Information units				Title
3.2.1.3a	Information type	D-T	D-T	D	
3.2.1.3b	Information format	D-T	D-T	D	
3.2.1.3.1	Information code				Title
3.2.1.3.1a	Abstract syntax	I	I	X	
3.2.1.3.1b	Transfer syntax	D-T	D-T	X	
3.2.1.3.1.1	Protocol Data Unit	D-T	D-T	X	

Table 4-1. Verification Requirements Traceability Matrix (cont.)

Section 3	Requirements	Verification Phase and Method			
		Sub-system Level	Integration Level	Site Level	Remarks
3.2.2.7	Subnetwork profile 1				Title
3.2.2.7a	Point-to-point protocols	I-T	D-T	D	
3.2.2.7.1	Dedicated connection				Title
3.2.2.7.1a	Initiate connection	D-T	D-T	D	
3.2.2.7.1b	Maintain connection	D-T	D-T	D	
3.2.2.7.1c	Disconnection	D-T	D-T	D	
3.2.2.7.2	Dial-up				Title
3.2.2.7.2a	Manager call	D-T	D-T	D	
3.2.2.7.2b	Agent authenticate	D-T	D-T	D	
3.2.2.7.2c	Agent call	D-T	D-T	D	
3.2.2.7.2d	Manager authenticate	D-T	D-T	D	
3.2.2.7.2e	Disconnection	D-T	D-T	D	
3.2.2.8	Subnetwork profile 2				Title
3.2.2.8a	LAN subnetwork protocols	D-T	D-T	D	
3.2.2.9	Subnetwork profile 3				Title
3.2.2.9a	WAN subnetwork protocols	D-T	D-T	D	
3.3	Security				Title
3.3a	Security requirements	D-T	D-T	D	

5. PREPARATION FOR DELIVERY

This section is not applicable to this IRD.

6. NOTES

6.1 Operational concept.

The purpose of this section is to identify the mission requirements pertinent to this interface and to provide an operational description of information interchange between the NAS Subsystem and the NIMS Manager.

6.1.1 NAS Infrastructure Management (NIM) operational concept.

Safe operation of the National Airspace System (NAS) depend on high availability and reliable performance of equipment and software. The operating philosophy of NIM is based upon managing the NAS infrastructure so that required services are provided to customers based on established performance standards, customer expectations and business objects.

6.1.1.1 NIM element mission requirements.

The NIM element consists of four sub-elements: the NAS Infrastructure Management System (NIMS), National Operations Control Center (NOCC), and Operation Control Center (OCC), and Work Centers (WC).

6.1.1.1.1 NIMS sub-element mission requirements.

The mission of NIMS is to provide remote performance monitoring and management of NAS infrastructure (systems, subsystems, and equipment and the services it provides. NIMS consists of two major components, managers and agents. The NIMS Manager will managed NAS subsystems remotely through NIMS Agents which monitor management data provided by the NAS subsystem. NIMS Managers will reside in the OCCs and NOCC, but may also reside in the WC in the future.

It is also the mission of the system to provide NIMS users with automated access to the management information collected by the NIMS Manager.

6.1.1.1.2 National Operational Control Center.

The NOCC is the organizational entity responsible for determining the overall status of the NAS on a continuous basis and implementing national operations priorities to ensure the smooth functioning of the NAS infrastructure. Specialists will utilize NIMS to monitor the NAS status from a national perspective and develop national and regional infrastructure strategies for short and long term planning purposes.

6.1.1.1.3 Operational Control Center.

The OCC is the organizational entity responsible for monitoring, managing, and maintaining services and equipment that are specific to the facility's area of responsibility. The OCCs, which will provide centralized managed of the NAS infrastructure is the result of the FAA transition from the decentralized Maintenance Control Center concept to the centralized Proto-type OCC concept.

The OCC will coordinate with the WC, adjacent OCCs, and the NOCC to implement national priorities. Specialists within the OCC will utilize NIMS to monitor and manage the NAS infrastructure from an area perspective and develop infrastructure strategies for short and long planning purposes.

6.1.1.1.4 Work Center.

The WC is the organizational entity responsible for working with their respective area OCC to maintain the infrastructure within their facility's area of responsibility. Where the system or facilities cannot be restored remotely, personnel from the WCs will travel to the site and perform necessary maintenance action to restore the system or facility to normal operation.

6.2 Definitions.

Agent: Entity capable of performing management operations on managed resources and emitting notifications on behalf of managed resources.

Attribute: A property of a managed resource.

Manager: Entity capable of issuing management operations and receiving notifications

Managed resource: Resources that may be managed through the use of management protocols.

Proxy agent: Entity capable of providing interface conversion with an non-standard agent to perform management operations on managed objects and emit notifications on behalf of managed objects.

6.3 Abbreviations and acronyms.

AP	Application Process
FAA	Federal Aviation Administration
CMIP	Common Management Information Protocol
IRD	Interface requirements documents
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
ISO	International Organization for Standardization
IPT	Integrated Product Team
LAN	Local area network
MCC	Maintenance Control Center
MIB	management information base
NADIN	National Data Interchange Network
NAS	National Airspace System
NIMS	NAS Infrastructure Management System
NOCC	National Operations Control Center
OCC	Operations Control Center
ORD	Operational requirements document
OSI	Open System Interconnection
OT&E	Operational test and evaluation
PDU	Protocol data unit
PSN	Packet switching network
PT	Product Team
SNMPv1	Simple Network Management Protocol Version 1
SNMPv2	Simple Network Management Protocol Version 2
VRTM	Verification Requirements Traceability Matrix
WC	Work Center